CLAIMS

1. A set-top-box (STB) comprising:

a databus;

a first communication device suitable for coupling to a digital broadcast communications medium, said first communication device operable to receive digital broadcast data;

memory bi-directionally coupled to said databus, said memory including computer executable instructions for:

a) determining whether said STB is authentic or counterfeit; and

b) performing anti-counterfeit measures upon said STB when said device is determined to be counterfeit;

a digital data decoder bi-directionally coupled to said databus;

a central processing unit (CPU) bi-directionally coupled to said databus, said CPU implementing a STB control process controlling said memory, said first communications device and said digital decoder, said STB control process operable to process digital data received at said first communications device.

2. A STB as recited in claim 1, wherein said memory includes transient random access memory (RAM) and a persistent storage device, and said computer executable instructions are stored on said persistent storage device.

3. A STB as recited in claim 2, wherein said persistent storage device is a hard disk.

4. A STB as recited in claim 1, further comprising an STB authenticity code hidden with the STB hardware, wherein said computer executable instructions for determining whether said STB is authentic or counterfeit includes a computer executable instruction for performing an integrity check upon said hidden STB authenticity code.

5. A STB as recited in claim 4, wherein said integrity check involves performing a cyclic redundancy check.

6. A STB as recited in claim 4, wherein said integrity check involves performing a checksum on said STB authenticity code.

7. A STB as recited in claim 4, wherein said integrity check involves querying a location wherein said STB authenticity code is hidden.

8. A STB as recited in claim 4, wherein said integrity check involves performing an image check upon said STB.

9. A STB as recited in claim 1, wherein said determining whether said STB is authentic or counterfeit involves performing an image check on the STB hardware.

10. A STB as recited in claim 4, wherein said performing anti-counterfeit measures upon said STB when said device is determined to be counterfeit includes disabling said STB.

11. A STB as recited in claim 4, wherein said performing anti-counterfeit measures upon said STB when said device is determined to be counterfeit includes damaging said STB.

12. A STB as recited in claim 4, wherein said performing anti-counterfeit measures upon said STB when said device is determined to be counterfeit includes transmitting a signal to a broadcast server site indicating that said STB is counterfeit.

13. A STB as recited in claim 12, wherein said signal includes information on the location of said STB.

14. A STB as recited in claim 1, wherein said memory further includes computer executable instructions for updating a communications protocol of said STB when said STB is determined to be authentic.

15. A STB as recited in claim 14, wherein said updating a communications protocol of said STB includes updating said communications protocol in order to enable said STB to

decode a broadcast signal encoded using an associated updated protocol.

16. A STB as recited in claim 15, wherein said broadcast signal encoded using said associated updated protocol is transmitted at a predetermined point in time.

17. A STB as recited in claim 16, wherein said STB is no longer able to decode broadcast signals encoded using the protocol used to encode broadcast signals transmitted before said predetermined point in time.

18. A STB as recited in claim 15, wherein said updating a communications protocol of said STB includes listening at a predetermined time and channel for a signal containing information for enabling said STB to decipher said updated protocol.

19. A STB as recited in claim 1, further comprising an STB authenticity code hidden with the STB software, wherein said computer executable instructions for determining whether said STB is authentic or counterfeit includes a computer executable instruction for performing an integrity check upon said hidden STB authenticity code.

20. A STB as recited in claim 18, wherein said updating a communications protocol of said STB includes altering at least a portion of said STB's existing communications protocol such that said STB is able to decipher signals transmitted using an updated communications protocol.

21. A STB as recited in claim 1, wherein said STB includes a graphic display device for displaying said digital broadcast data.

22. A set-top-box (STB) comprising:

a databus;

a first communication device suitable for coupling to a digital broadcast communications medium, said first communication device operable to receive digital broadcast data;

memory bi-directionally coupled to said databus, said memory including computer

executable instructions for:

a) determining whether said STB is authentic or counterfeit;

b) performing anti-counterfeit measures upon said STB when said device is determined to be counterfeit; and

c) updating a communications protocol of said STB when said STB is determined to be authentic;

a digital data decoder bi-directionally coupled to said databus;

a central processing unit (CPU) bi-directionally coupled to said databus, said CPU implementing a STB control process controlling said memory, said first communications device and said digital decoder, said STB control process operable to process digital data received at said first communications device.

23. A STB as recited in claim 22, wherein said memory includes transient random access memory (RAM) and a persistent storage device, and said computer executable instructions are stored on said persistent storage device.

24. A STB as recited in claim 23, wherein said persistent storage device is a hard disk.

25. A STB as recited in claim 22, further comprising an STB authenticity code hidden with the STB hardware, wherein said computer executable instructions for determining whether said STB is authentic or counterfeit includes a computer executable instruction for performing an integrity check upon said hidden STB authenticity code.

26. A computer implemented method for authenticating validity of a data receiving system such as a set-top-box, said computer implemented method comprising the act of:

transmitting to said data receiving system an anti-counterfeit software application executable by said data receiving system, said anti-counterfeit software operable to determine whether said data receiving device is counterfeit or authentic, said anti-counterfeit software further operable to perform anti-counterfeit measures at said data receiving system.

27. A method as recited in claim 26, wherein said data receiving system includes a communications protocol for deciphering data signals and when said data receiving system is determined to be authentic, said anti-counterfeit software application being further operable to update said communications protocol.

28. A method as recited in claim 27, wherein said anti-counterfeit software application is further operable to send a message to a predetermined location.

29. A method as recited in claim 28, wherein said sending a message is sent via the internet.

30. A method as recited in claim 28, wherein said predetermined location is a bi-directional DOD server.

31. A method as recited in claim 28, wherein said message is sent via a telephone connection.

32. A method as recited in claim 28, wherein said message is sent via a broadband connection.

33. A method as recited in claim 28, wherein said message is sent via a cable modem.

34. A counterfeit counter measure for transmission signal processors comprising:
a transmission signal;
an authenticity checker that is embedded in said transmission signal;
a transmission signal processor;
an authenticity verification that is embedded in said transmission signal processor;
wherein said authenticity checker executes once received by said transmission signal processor;
wherein said authenticity checker searches said transmission signal processor for said authenticity verification;

wherein if said authenticity verification is found said transmission signal processor processes said transmission signal properly; and

wherein if said authenticity verification is not found said transmission signal processor is disabled.

35. The counterfeit counter measure for transmission signal processors of claim 34, wherein said authenticity checker is embedded in a protocol update.

36. The counterfeit counter measure for transmission signal processors of claim 34, wherein said authenticity verification is software.

37. The counterfeit counter measure for transmission signal processors of claim 34, wherein said authenticity checker is hardware.

38. The counterfeit counter measure for transmission signal processors of claim 34, wherein when said transmission signal processor no longer functions properly is due to failure of said transmission signal processor to properly process said transmission signal.

39. The counterfeit counter measure for transmission signal processors of claim 34, wherein when said transmission signal processor no longer functions properly due to said transmission signal processor malfunctioning.

40. The counterfeit counter measure for transmission signal processors of claim 34, wherein said transmission signal is part of a uni-directional transmission system.

41. The counterfeit counter measure for transmission signal processors of claim 34, wherein said transmission signal is part of a bi-directional transmission system.

42. The counterfeit counter measure for transmission signal processors of claim 41, wherein if said authenticity verification is not found, an additionally a signal is sent back to the source of said transmission signal.

43. A set-top box (STB) that receives a data file in data blocks for uni- and bi-directional signal system with a counterfeit countermeasures comprising:

a STB that is incorporated with a data file utilizing device;

a counterfeit countermeasure incorporated with said STB, said counterfeit countermeasure comprising an authenticity verification;

a signal source linked to said STB;

a data file that is broken into data blocks and sent over said signal source to said STB;

an authenticity checker embedded in said data file;

wherein said data is transmitted to said STB;

wherein once said data file is transmitted to said STB, said authenticity checker searches said STB for said authenticity verification; and

wherein if said authenticity verification is found, said data file may be restored from said data blocks and used by said data file utilizing device.

44. The set-top box (STB) that receives a data file in data blocks for uni- and bi-directional signal system with a counterfeit countermeasures according to claim 43, wherein said authenticity checker embedded in said data file is further embedded in a protocol update portion of said data file.